SneakyChef espionage group targets government agencies with SugarGh0st and more infection techniques

Chetan Raghuprasad ⋮⋮ 6/21/2024

By Chetan Raghuprasad, Ashley Shen

Friday, June 21, 2024 08:00
Threats RAT

- Cisco Talos recently discovered an ongoing campaign from SneakyChef, a newly discovered threat actor using SugarGh0st malware, as early as August 2023.
- In the newly discovered campaign, we observed a wider scope of targets spread across countries in EMEA and Asia, compared with previous observations that mainly targeted South Korea and Uzbekistan.
- SneakyChef uses lures that are scanned documents of government agencies, most of which are related to various countries' Ministries of Foreign Affairs or embassies.
- Beside the two infection chains disclosed by Talos in November, we discovered an additional infection chain using SFX RAR files to deliver SugarGh0st.
- The language used in the SFX sample in this campaign reinforces our previous assertion that the actor is Chinese speaking.

Cisco Talos would like to thank the Yahoo! Paranoids Advanced Cyber Threats Team for their collaboration in this investigation.

SneakyChef actor profile

In early August 2023, Talos discovered a campaign using the SugarGh0st RAT to target users in Uzbekistan and South Korea. We continued to observe new activities using the same malware to target users in a wider geographical location. Therefore, we created an actor profile for the group and dubbed them "SneakyChef."

Talos assesses with medium confidence that SneakyChef operators are likely Chinese-speaking based on their language preferences, the usage of the variants of Gh0st RAT — a popular malware among various Chinese-speaking actors — and the specific targets, which includes the Ministry of Foreign affairs of various countries and other government entities. Talos also discovered another RAT dubbed "SpiceRAT" used in the campaign. Read the corresponding research here.

ACTOR PROFILE **SneakyChef**	
Aliases	Unknown
Affiliations	Chinese-Speaking actor
Active since	2023
Goals	Espionage and data theft
Victimology	Government entities and private sectors in EMEA and Asia
Notable TTPs	Spear-Phishing campaign, DLL Side-Loading, custom c2 communication protocol, abusing the legitimate applications
Malware & tooling	SugarGh0st, SpiceRAT and plugin

Targets across EMEA and Asia
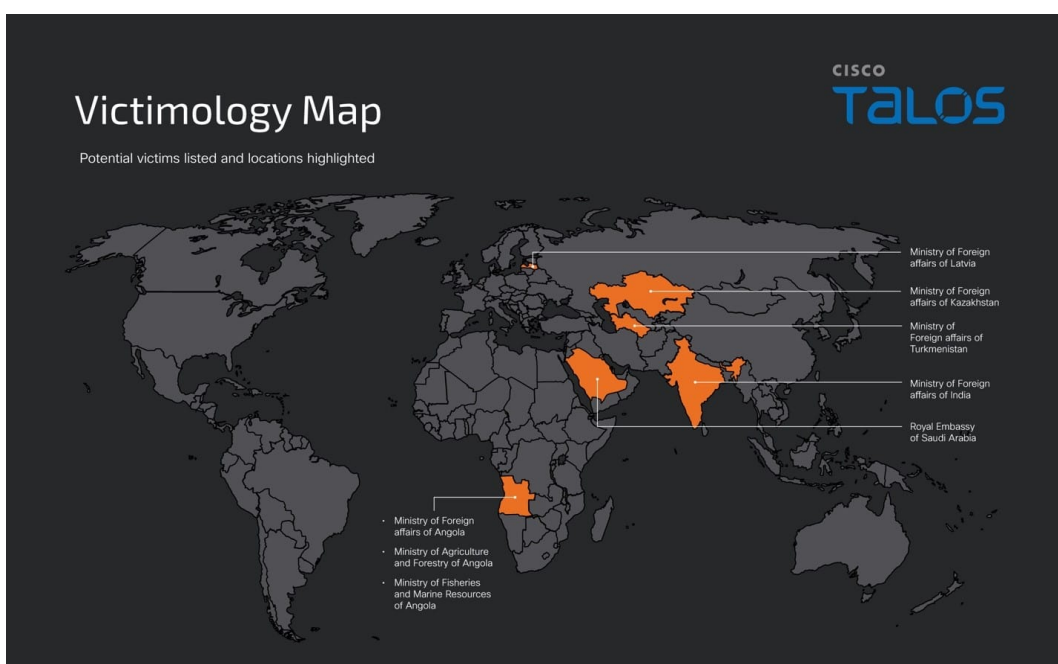
Talos assess with low confidence that the following government agencies are the potential targets in this campaign based on the contents of the decoy documents:

- Ministry of Foreign affairs of Angola
- Ministry of Fisheries and Marine Resources of Angola
- Ministry of Agriculture and Forestry of Angola
- Ministry of Foreign affairs of Turkmenistan
- Ministry of Foreign affairs of Kazakhstan
- Ministry of Foreign affairs of India
- Embassy of the Kingdom of Saudi Arabia in Abu Dhabi
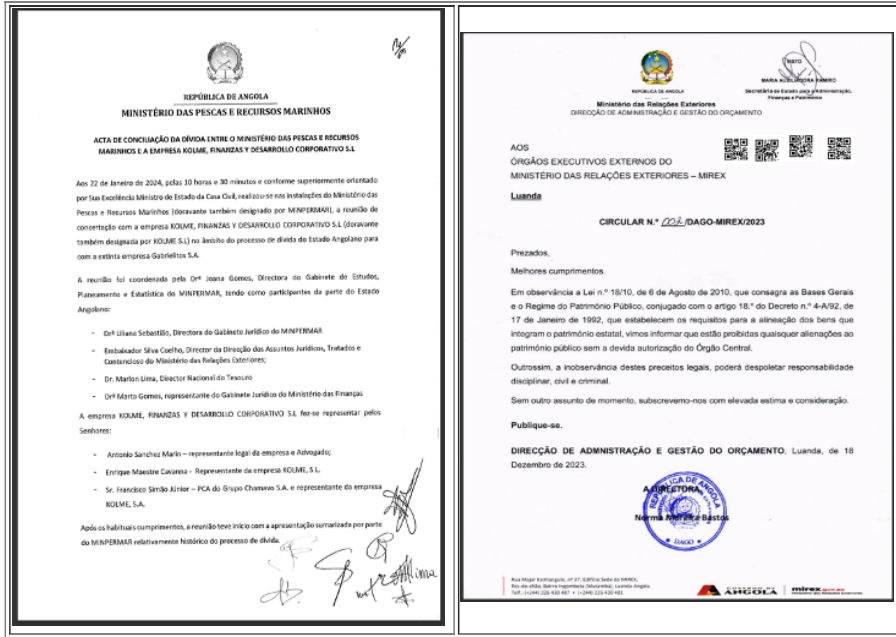- Ministry of Foreign affairs of Latvia

Most of the decoy documents we found in this campaign are scanned documents of government agencies, which do not appear to be available on the internet. During our research, we observed and analyzed various decoy documents with government-and research conference-themed lures in this campaign. We are sharing a few samples of the decoy documents accordingly.

Lures targeting Southern African countries

The threat actor has used decoy documents impersonating the Ministry of Foreign affairs of Angola. The lure content in one of the sample documents appeared to be a circular from the Angolan Ministry of Fisheries and Marine

Resources about a debt conciliation meeting between the ministry authority and a financial advisory company.

Another document contained information about a legal decree concerning state or public assets and their disposal. This document appealed to anyone interested in legal affairs and public heritage regimes and was addressed to the Ministry of Foreign Affairs – MIREX, a centralized institution in Luanda.

Lures targeting Central Asian countries

The decoy documents used in the attacks likely targeting countries in Central Asia were either impersonating the Ministry of Foreign affairs of Turkmenistan or Kazakhstan. One of the lures is related to a meeting organized with the Turkmenistan embassy in Argentina and the heads of transportation and infrastructure of the Italian Republic. Another document was a report of planned events and the government-issued list of priorities to be addressed in the year 2024 that includes a formal proclamation-signing event between the Ministry of Defense of Uzbekistan and the Ministry of Defense of Kazakhstan.
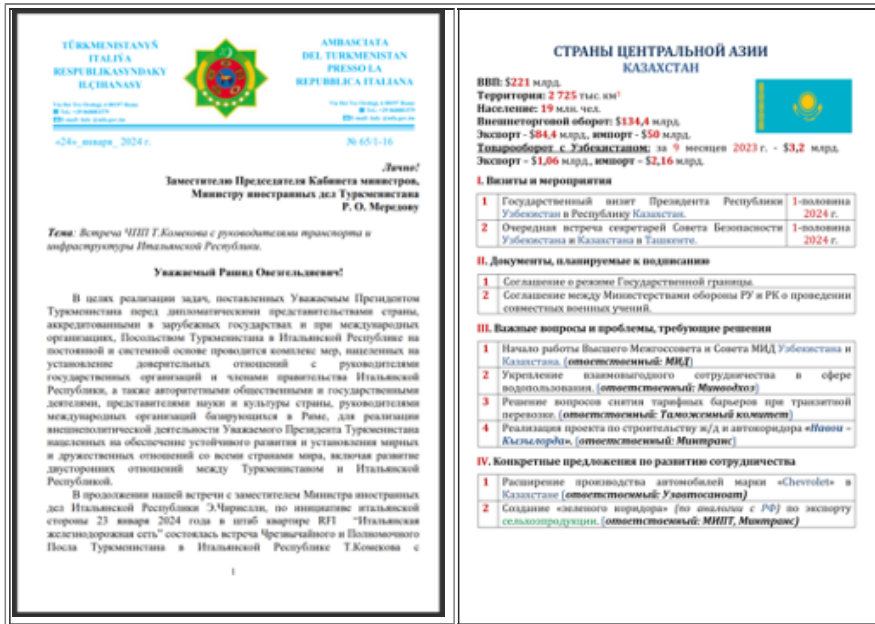

Lures targeting Middle Eastern countries

A decoy document we observed in the attack likely targeting Middle Eastern countries was an official circular regarding the declaration of an official holiday for the Founding Day of the Kingdom of Saudi Arabia.

Lures targeting Southern Asian countries

We found another sample that was likely used to target the Indian Ministry of Foreign Affairs. It has decoy documents, including an Indian passport application form, along with a copy of an Aadhar card, a document that serves as proof of identity in India.
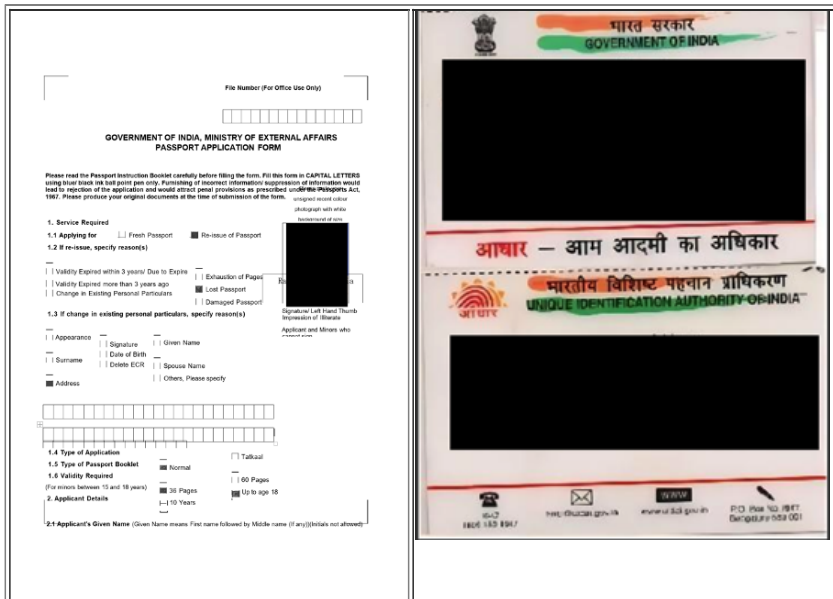
One of the decoy Word documents we observed contained lures related to India-U.S. relations, including a list of events involving interactions between India's prime minister and the U.S. president.

India-US Bilateral Relations – A Brief

India and United States enjoy a comprehensive global strategic partnership covering almost all areas of human endeavor, driven by shared democratic values, convergence of interests on a range of issues, and vibrant people-to-people contacts.

High-Level Exchanges

2. Regular dialogue between the Leaders is an important element of the expanding bilateral ties. The outcomes of these visits have been instrumental in strengthening the multifaceted bilateral ties.

3. There is regular high-level interaction between Prime Minister Shri Narendra Modi and President Biden with regular meetings. Prime Minister also participated in virtual Summits convened by President Biden including Quad, I2U2 (India, Israel, USA and UAE), Summit for Democracy and other events.

4. **PM's interactions with President Biden:**
   - G7 and Quad Leaders Summit, 20 May 2023 in Hiroshima, Japan
   - Telephonic conversation on 14 February 2023
   - Virtual Summit for Democracy on 29 March 2023
   - Sidelines of G20 Summit in Bali on 15 November 2022
   - G7 Summit in Germany on 27 June 2022.
   - Quad Leaders' Summit in Tokyo, Japan on 24 May 2022 including a bilateral meeting.

5. PM Modi made his first State Visit to the US from 21-23 June 2023 at the invitation of President Biden. In addition to a bilateral meeting with President Biden, he addressed a Joint Meeting of US' Congress and interacted with business and thought leaders. PM Modi had visited the US in September 2021 for the first in-person Quad Leaders' Summit on 24 September 2021.

6. President Biden visited New Delhi from 7-10 September 2023 to attend G-20 Leaders' Summit. President Biden and PM Modi had a bilateral meeting on 8 September 2023. The two Leaders also co-hosted a group of G20 leaders on 9 September 2023 to accelerate investments in high-quality infrastructure projects and development of economic corridors through the India Middle East Europe Economic Connectivity Corridor and the Partnership for Global Infrastructure and Investment (PGI).

Lures targeting European countries

A decoy document found in a sample likely targeting the Ministry of Foreign Affairs of Latvia was a circular impersonating the Embassy of Lithuania. It contained a lure document regarding an announcement of an ambassador's absence and their replacement.

Other targets

Along with the government-themed decoy document samples we analyzed, we observed a few other samples from these campaigns. These included decoys such as an application form to register for a conference run by the Universal Research Cluster (URC) and a research paper abstract of the ICCSE international conference. We also saw a few other decoys related to other conference invitations and details, including those for the Political Science and International Relations conference.

Recently, Proofpoint researchers reported a SugarGh0st campaign targeting an organization in the U.S. involved in artificial intelligence across academia, the private technology sector, and government services, highlighting the wider adoption of SugarGh0st RAT in targeting various business verticals.

Threat actor continues to leverage old and new C2 domains

After Talos' initial disclosure of SugarGh0st campaign in November 2023, we are attributing the past attacks to the newly named threat actor SneakyChef. Despite our disclosure, SneakyChef continued to use the C2 domain we mentioned and deployed the new samples in the following months after our blog post. Most of the samples observed in this campaign communicate with the C2 domain account[.]drive-google-com[.]tk, consistent with their previous campaign. Based on Talos' Umbrella records, resolutions to the C2 domain were still observed until mid-May.

DNS requests for the SugarGh0st C2 domain.

Talos also observed the new domain account[.]gommask[.]online, reported by Proofpoint as being used by SugarGh0st. The domain was created in March 2024, and queries were observed through April 21.

Infection chain abuse SFX RAR as the initial attack vector

With Talos' first reporting of the SugarGh0st campaign in November, we disclosed two infection chains that utilized a malicious RAR with an LNK file, likely delivered via phishing email. In the newly observed campaign, in addition to the old infection chains, we discovered a different technique from a few malicious RAR samples.
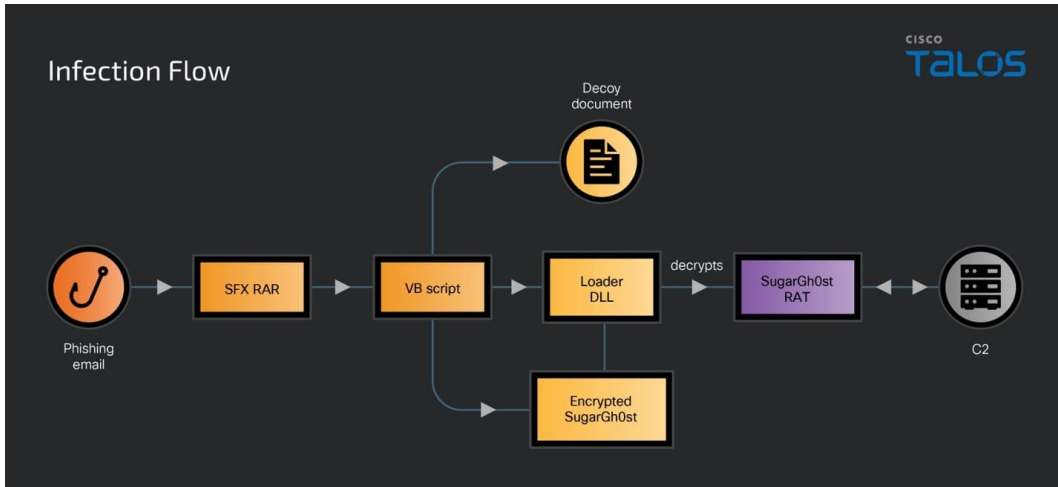
The threat actor is using an SFX RAR as the initial vector in this attack. When a victim runs the executable, the SFX script executes to drop a decoy document, DLL loader, encrypted SugarGh0st, and a malicious VB script into the victim's user profile temporary folder and executes the malicious VB script.
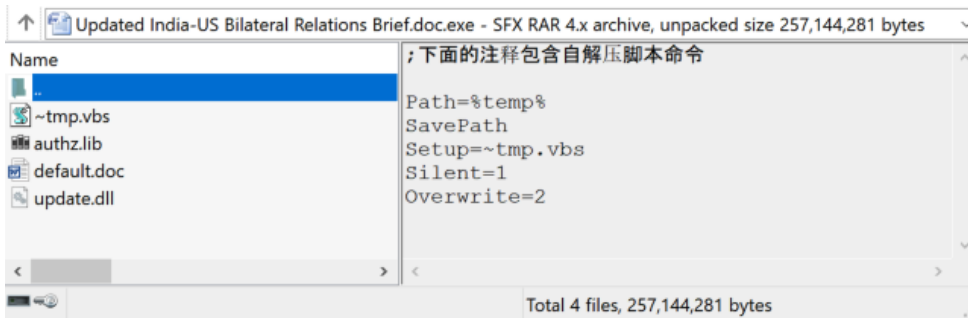
The malicious VB script establishes persistence by writing the command to the registry key UserInitMprLogonScript which executes when a user belonging to either a local workgroup or domain logs into the system.

Registry key	Value
HKCU\Environment\UserInitMprLogonScript	regsvr32.exe /s %temp%\update.dll

```
on Error Resume next
set obj=wscript.createObject("wscript.shell")
obj.RegWrite "HKCU\Environment\UserInitMprLogonScript","regsvr32.exe /s %temp%\update.dll"
obj.run "%temp%\default.doc",1
```

When a user logs into the system, the command runs and launches the loader DLL "update.dll" using regsvr32.exe. The loader reads the encrypted SugarGg0st RAT "authz.lib", decrypts it and injects it into a process. This technique is same as that of the SugarGh0st campaign disclosed by the Kazakhstan government in February.

Indicators of Compromise

Indicators of Compromise associated with this threat can be found here